ABA BUSINESS LAW SECTION

KNOWLEDGE | COMMUNITY | EXPERIENCE

Volume 14, Number 2 - November/December 2004

Hey, that's personal!

When companies sell customer information gathered through the Internet

By Bethany Rubin Henderson

Imagine this: A new customer walks into your client's place of business. Within minutes your client knows *all* about that customer.

So what exactly is "all"? That would be his tastes and interests, how he prefers to shop (such as whether he browses the store at length or goes straight to the desired product), his purchasing habits, how he prefers to interact with your client's company (such as whether he reads posted signs and how he prefers to communicate with sales associates), what he is willing to pay for your client's products or services, and his contact information. Your client finds out all of this before the customer says a single word, and without the customer knowing that your client is gathering this information. Instantly — and without the customer even realizing it — your client's store morphs into an environment personalized entirely for that customer.

The result: an enormous boon to your client's bottom line. Sound unrealistic? In the bricks and mortar world, absolutely. However, thanks to Internet technology, any company with a Web site can do this. Many already are.

Sure, you may say, that sounds wonderful, but how can that be lawful? With all of the press about identity theft these days, and federal legislation such as the 2003 USA Patriot Act and Homeland Security Act, there must be laws prohibiting my client from surreptitiously gathering and using such information. Surprisingly, very few such laws are on the books.

However, a legal regime is slowly developing, and the Federal Trade Commission

and certain states recently have begun taking a very active role in ensuring compliance with fair information practices. This article reviews what every in-house counsel and business lawyer should know about commercial clients' collection, use and sale of the personally identifiable information of online customers.

Web sites that do not cull their visitors' information may be at a distinct disadvantage in the marketplace. The vast majority of companies with Web sites *do* collect personally identifiable information from online visitors, and, according to a recent FTC study, more than two-thirds collect nonpersonally identifiable information as well. Some of the more common methods used to collect such information are:

- *Requesting it voluntarily* — Most Web sites require that visitors who purchase goods or services take part in online contests or surveys, or who register to use a Web site or an online service voluntarily provide contact and billing information. It is becoming increasingly common in some industries to require a visitor to provide contact information, or at least to register a username and password, before allowing her to even browse a Web site.

  Many sites request far more information than is required for any particular transaction, and all but the savviest Internet users usually willingly provide it. It is increasingly common for Web sites to offer visitors the choice to opt out of certain uses of their personal data, but many visitors do not bother to change a default setting of opting in;
- *Spyware* — There are various types of software that may be placed on a Web site visitor's computer, without his knowledge, to transmit information about the Internet habits and interests of that computer's users back to the company that installed the device. Two of the most common and well-known tracking devices are Web bugs (graphic image files embedded in a Web page that are invisible to the naked eye) and cookies (files sitting on a computer's hard drive); and
- *Tracking clickstreams* — Certain types of software and spyware programs enable companies to track the pattern and order of visitors' mouse movements and clicks within and across Web sites.

It is common to use multiple data-gathering tools simultaneously. These technologies, especially when used in conjunction with each other, make it possible to track a Net user's online behavior over an extended period of time, often regardless of whether she knows of or consents to the collection of that information, and even if she logs on and off the Internet or periodically shuts down and re-starts her computer.

More important, they allow the easy correlation of individual Web site visitors' personally identifiable information with nonpersonally identifiable information. These compilations can be used to create profiles of individual Internet users, which can be highly valuable. For example, such profiles may be used, among other things:

- to predict a Web site visitor's interests and purchasing habits, thereby making it possible to target ads, prices and content directly to that individual;
- for internal market research and development;
- for direct profit by selling customer lists, information and preferences to third parties; and
- to market other products or services.

Industry and third-party privacy organizations have rushed to fill the void left by the dearth of federal legislation concerning online consumer privacy. For many years, the FTC supported industry self-regulation and took little direct action itself against companies that abused customer data they collected online. As a result, several industry organizations created their own standards for their members' online collection and use of consumers' personally identifiable information.

Additionally, numerous third-party seal programs purport to independently monitor Web sites' information collection and use practices. Seal programs typically offer a branded privacy seal and public recognition to those Web sites that abide by their recommended privacy practices. *(See sidebar on*

third-party privacy guidelines.)

Self regulation and third-party regulation has proven to be relatively ineffective because the rules governing the use of personally identifiable information are not uniform. Although virtually all of the third-party privacy guidelines center on the commonly accepted fair information practice principles of notice, choice, access and security, each program has developed its own distinct — and often-competing — set of rules particular to its own membership and goals.

Many companies also create their own unique privacy practices, which may be inconsistent with those recommended by industry or third-party privacy organizations. Consequently, the online collection and use of personally identifiable information is inconsistent even within industries.

Furthermore, enforcement of these self-imposed guidelines is greatly limited. Most industry-promulgated and third-party guidelines have minimal enforcement mechanisms. Commercial entities are not required to join privacy seal programs, and compliance with internal privacy policies depends largely on self-reporting. In short, without the threat of legal sanctions, companies have little to no incentive to audit their adherence to any privacy practices.

The FTC recognized these shortcomings and recently has reversed its long-held position that online consumer privacy protection should be left to industry self- regulation. The FTC has begun to hold forums on topics such as spyware and to issue public opinion letters about various online consumer privacy issues and practices. Over the last five years, the FTC also has started pursuing litigation and administrative actions against companies that egregiously abuse customers' privacy or deceptively collect or use online consumers' personally identifiable information.

The FTC has prosecuted several different companies (most recently Tower Records) for permitting security flaws in their Web sites and computer systems that made consumers' personally identifiable information vulnerable to exposure to third parties in violation of those companies' privacy policies. The FTC also has pursued actions against numerous companies for deceptively collecting, using and selling personally identifiable information from online consumers, as well as for making false statements about online information collection practices and security.

For example, the FTC recently prosecuted Gateway Learning, best known for its "Hooked on Phonics" products, for engaging in unfair and deceptive trade practices related to its renting of online customers' personally identifiable information to third-party marketers. See *In the Matter of Gateway Learning Corp.*,FTC File No. 042-3047. GeoCities, ToySmart.com, Microsoft and Guess.com also have been recent targets of the FTC's crackdown on corporate abuse or misuse of online consumers' personally identifiable information.

The case of Gateway Learning is particularly instructive. Gateway Learning collected personally identifiable information from online consumers under a privacy policy that expressly promised that collected information would not be sold, and that consumers would be given the opportunity to opt out of any future sale if the policy changed.

Nevertheless, in 2003, Gateway Learning began to rent out customers' information to third-party marketers, and changed its privacy policy retroactively to permit such activities, without notifying its consumers or obtaining their consent. The FTC charged Gateway Learning with violating Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices.

In July 2004, the parties reached a settlement agreement that, among other things, bars Gateway Learning from sharing any online customer's personal information without affirmative opt-in consent, prohibits Gateway Learning from retroactively changing its privacy policy without customer consent, and

requires Gateway Learning to relinquish all profits from the rental of its online customers' information.

Neither federal nor state legislation has caught up with the FTC. Today there still is no unified regulatory scheme governing what sort of personally identifiable information lawfully can be collected online (or offline) by commercial entities or how such information can be used or disseminated after it is collected. The federal legislation that does regulate what commercial entities may do with consumer information is piecemeal and typically focuses on a particular type of personally identifiable information or a particular use of that information. For example, multiple statutes regulate identity theft, and several new bills on that subject were introduced in the 108th Congress (such as S.153, S.223, H.R.1731 & H.R.2035).

Industry-specific legislation restricting the use and dissemination of certain types of personal information also abounds. *(See the sidebar on industry-specific federal legislation.)* Although Congress has so far taken only a piecemeal approach to protecting consumer privacy, these disparate statutes and bills, taken together, show Congress' willingness both to protect individual privacy and to punish those who fail to respect the awesome responsibility that comes with the possession of personally identifiable information.

Recently, Congress has begun to recognize that Internet technology poses new challenges to personal privacy that cannot be sufficiently circumscribed by the existing piecemeal legislation. To date, only two federal laws directly address the Internet environment and regulate the collection and use of personally identifiable information gathered from Web site visitors. Although debate rages about the efficacy and enforceability of both statutes, they demonstrate Congress' willingness to legislate in the online arena.

One of those statutes is the Children's Online Privacy Protection Act, 15 U.S.C. §6501 (1998) (COPPA). COPPA restricts both Web sites targeted at children younger than 13, and those who knowingly collect information online from such children, from collecting and using children's personally identifiable information without verifiable parental consent.

The other statute is the Controlling the Assault of Non- Solicited Pornography and Marketing Act, 15 U.S.C. 7701 (2003) (CAN-SPAM Act). CAN-SPAM focuses primarily on regulating the identification and transmission of unsolicited marketing and sexually explicit e-mails. However, it also contains restrictions on the gathering and use of personal e-mail addresses. CAN-SPAM requires that conspicuous notice be given to e-mail recipients on how to opt out of receiving e-mails, and prohibits e- mailing those who do opt out.

It forbids knowingly sending commercial e-mails to addresses collected by Web sites with privacy notices stating that the Web-site operator will not disseminate e-mail addresses it collects. CAN-SPAM also proscribes knowingly sending commercial e-mails to addresses identified through automated harvesting (that is, combining names, letters or numbers in various permutations through automated means). Violations of both COPPA and the CAN-SPAM Act are explicitly deemed unfair and deceptive trade practices under the Federal Trade Commission Act.

To date, no single federal law regulates what companies can do with the other personally identifiable information they gather from *adult* Internet users. However, the absence of such legislation should not be seen as suggesting that Congress is not interested in this particular subject. In fact, in each of the last several sessions of Congress, multiple bills specifically targeted at restricting the collection, use and sale of information gathered online were introduced in both houses.

During the 107th Congress, several bills in both houses aimed to regulate the online collection and use of personally identifiable information. The broadest ones were the Senate's Online Privacy Protection Act (S.2201) and the House of Representatives' Consumer Privacy Protection Act of 2002 (H.R. 4678). The

Senate bill explicitly recognized the unique dangers to privacy posed by the Internet, while the House bill addressed consumer privacy generally. Both bills provided for enforcement by the FTC. The Senate bill also authorized limited private and state actions for certain violations. However, neither bill made it very far. The Senate bill was placed on the Senate calendar, but no action was ever taken on it. The House bill never even made it out of committee.

Many more bills addressing the use and dissemination of personally identifiable information have been introduced in the 108th Congress to date. Restricting commercial installation and use of spyware — which is viewed as particularly insidious by many legislators and privacy advocates — has been a favorite subject of recent legislative proposals. In fact, in October the House passed two separate anti-spyware bills, which are now awaiting review by the Senate. (H.R.4661 and H.R. 2929). Restrictions on the collection and commercial use of distinct types of personally identifiable data, including Social Security numbers and TV viewing preferences, also has remained popular in the 108th Congress.

While most of the legislative proposals in Congress target specific types or uses of personal data, four bills broadly aim to restrict the collection and use of online or electronic data. Those bills are:

- Privacy Act of 2003 (S.745): seeks to prohibit commercial entities from disclosing or selling to third parties any personally identifiable customer information collected either online or offline without first notifying those individuals whose information has been collected and providing them adequate opportunity to restrict or opt out of the sale of their information;
- Online Privacy Protection Act of 2003 (H.R.69): proposes restrictions on the online use and collection of personally identifiable information of persons not covered by COPPA;
- Notification of Risk to Personal Data Act (S.1350): seeks to require those engaged in interstate commerce to disclose the unauthorized acquisition of electronic data containing personal information; and
- Consumer Privacy Protection Act of 2003 (H.R.1636): a comprehensive bill with language broadly aimed at protecting personally identifiable information in a variety of contexts.

Despite the abundance of recent legislative proposals about online consumer privacy, none of the proposed bills has advanced to a full floor vote. In fact, most have languished in committee. However, the various proposals share many similarities with each other, with COPPA, and with those portions of the CAN-SPAM Act regulating the collection, sale and use of personal e- mail addresses. Taken together they provide a roadmap to what sort of regulations Congress may impose on the online collection and use of adults' personally identifiable information.

First, they generally direct that adequate and accurate notice be given to those persons whose information is being collected about how that information will be collected, used and disseminated. Second, they generally require that the individual whose data is at issue consents to its collection and use. Most commonly, the proposed bills approve the use of opt-out mechanisms to accomplish this feat. Finally, and most important, these bills provide for meaningful enforcement mechanisms.

Virtually all of the proposed legislation explicitly lodges enforcement authority in the FTC. Most of the bills explicitly classify violations of their provisions as violations of the unfair and deceptive trade practices provisions of the Federal Trade Commission Act. One, the Privacy Act of 2003 (S.745), also contains a safe harbor provision excluding from its mandate those commercial entities that comply with FTC-approved self- regulatory guidelines issued by industry or third-party privacy seal organizations. Some proposed bills also expressly grant states or private individuals limited rights to pursue civil actions for certain violations.

The volume of legislation proposed in the 107th and 108th Congresses that was directed at commercial entities' online collection, use and dissemination of personally identifiable information suggests that federal legislation on these topics may well be coming. The similarities in those bills reveal that the FTC

is likely to be the primary enforcement authority and that the Federal Trade Commission Act's prohibition against unfair and deceptive trade practices likely will set the standard by which companies' actions will be measured.

Further, the FTC's stepped-up activities — despite the absence of federal legislation — coupled with recent actions by states such as New York, Texas and Michigan against private companies that violate their own online data collection privacy policies or abuse the privacy of online consumers, demonstrate that commercial entities engaging in the online collection, use and dissemination of personally identifiable information should be circumspect.

This does not mean that companies should stop collecting and using such data. In fact, personally identifiable data is so valuable that any commercial entity that does not take advantage of every opportunity to collect and use such information is likely to quickly find itself at a competitive disadvantage. However, at a minimum, companies can and should adhere to standard fair information practice guidelines to protect themselves from future litigation or hefty penalties.

Third-party privacy guidelines

Industry organizations with online consumer privacy guidelines include:

- *Online Privacy Alliance*: a cross-industry coalition of nearly 100 global companies. (http://www.privacyalliance.org)
- *Network Advertising Initiative*: an organization of companies that facilitate Web advertising through ad serving, hosting and ad sales services. (http://www.networkadvertising.org)
- *Direct Marketing Association*: the trade organization for direct marketers. (http://www.the-dma.org/privacy/index.shtml)

Some of the more widely recognized third-party seal programs are:

- The Better Business Bureau Online (https://www.bbbonline.org/privacy)
- TRUSTe(http://www.truste.org)
- PrivacyBot (http://www.privacybot.com)

Industry-specific federal legislation

Federal legislation targeting consumer privacy crosses virtually every industry. Some of the more prominent federal statutes restricting what companies can do with customers' personally identifiable data are:

- Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701: prohibits electronic communication service providers from disclosing the contents of the electronic communications stored on their servers.
- Cable Communications Policy Act, 47 U.S.C. §551: regulates cable television companies' collection and use of customers' personal data.
- Video Privacy Protection Act, 18 U.S.C. §2710: restricts disclosure of customers' personal information and video rental practices and preferences by videotape sale or rental companies.
- Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.*: regulates the collection and use of consumer credit information.
- Gramm-Leach-Bliley Act, 15 U.S.C. §6801 *et seq.*: regulates the disclosure of nonpublic personal information by financial institutions.
- Health Insurance Portability and Accountability Act of 1996: regulates the collection, use and dissemination of patients' medical records and information.

Best practices

Have a transparent and conspicuous privacy policy that is readily accessible to Web site visitors, and strictly adhere to it;

- Notify customers whose information has been collected in advance of any material changes to your privacy policy and give them the opportunity either to opt out of the changes or to delete their personally identifiable information from your database;
- Join an independent seal program and adhere to its privacy practices;
- Provide a meaningful mechanism for visitors to opt out of having their information either collected while browsing your Web site or used in particular ways, and scrupulously honor all opt-out requests;
- Maintain personal data collected online in a secure environment in accordance with a clear privacy policy, and repeatedly review and update security mechanisms to ensure that no vulnerabilities exist; and
- Do not sell a Web site visitor's personally identifiable information to third parties without either the visitor's express prior permission or without making an explicit and conspicuous public announcement of your intentions and providing a meaningful opt-out mechanism.

— Bethany Rubin Henderson

Henderson is an associate at Quinn Emanuel Urquhart Oliver & Hedges, LLP, in Los Angeles. Her e-mail is bethanyhenderson@quinnemanuel.com.

Back to Top

